This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2025.3620040

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Digital Object Identifier 10.1109/ACCESS.2024.Doi Number

Symbolic Plithogenic numbers in RSA cryptography: a path to post-quantum security

MEHMET MERKEPÇİ [1], HAMİYET MERKEPÇİ [2], and ALEXANDRA IOANID [3,4]

[1]Department of Computer Engineering, Gaziantep University, Gaziantep 27310 TÜRKİYE
[2]Department of Mathematics, Gaziantep University, Gaziantep 27310 TÜRKİYE
[3]Department of Entrepreneurship and Management, National University of Science and Technology Politehnica Bucharest, Splaiul Independentei 313, Bucharest, Romania, alexandra.ioanid@upb.ro
[4] Academy of Romanian Scientists, Ilfov 3, 050044 Bucharest, Romania

ABSTRACT The RSA algorithm, with its strong mathematical foundation rooted in number theory and its wide range of applications in secure communication, is one of the most widely used public-key encryption methods. However, advancements in classical computing and the emergence of quantum computers have introduced significant risks that threaten the security of traditional RSA-based systems. Therefore, new mathematical structures, referred to as extended number systems, are needed to increase algebraic complexity and provide more secure encryption. In this context, alternative number systems such as neutrosophic numbers and plithogenic numbers, which possess multidimensional and partially ordered structures, show promising potential for offering stronger cryptographic solutions against both classical and quantum-based attacks. This study presents a reconstruction of the RSA algorithm using symbolic 2-plithogenic and 3-plithogenic numbers, which represent an extended version of the classical and neutrosophic number systems. These numbers differ from traditional integers by incorporating two symbolic components, thereby forming a multidimensional structure. Consequently, the algebraic structure obtained in the processes of encryption and key generation becomes significantly more complex compared to classical methods. In particular, the increased difficulty of integer factorization in such multidimensional structures substantially strengthens cryptographic security.

INDEX TERMS Cryptography, Decryption, Encryption, RSA, Symbolic plithogenic numbers, public key, Private key.

I. INTRODUCTION

In today's digital era, where information holds strategic value, ensuring confidentiality, integrity, and authenticity of data has become one of the essential requirements of modern communication infrastructures. In this context, cryptology comprising the disciplines of encryption (cryptography) and decryption (cryptanalysis) serves as the scientific foundation for secure data transmission and information protection mechanisms. Cryptography involves the development of mathematical methods designed to ensure that only authorized users can access specific information. Although symmetric key algorithms offer advantages in terms of speed and efficiency, they present various security risks due to the need for secure key exchange. To address this issue, asymmetric key encryption methods have developed, among which the RSA algorithm proposed by Rivest, Shamir, and Adleman in 1977 has become a cornerstone of public key cryptography [1].

The RSA algorithm is built upon a robust mathematical structure grounded in number theory. Its security relies on the computational difficulty of factoring a number that is the product of two large prime numbers, which is infeasible to perform efficiently using classical computers. The system is based on encryption with a public key and decryption with a private key. Mathematical concepts such as Euler's totient function, modular arithmetic, and modular inverse computations constitute the fundamental components of the algorithm. Despite its theoretically simple structure, when implemented correctly, the RSA algorithm provides a high level of security. For this reason, RSA is effectively used in secure communication today.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2025.3620040

The RSA algorithm is utilized in a wide range of areas, including digital signature generation, secure e-mail communication, security protocols, and blockchain applications. Paar and Pelzl uniquely designed a book about cryptograpy for students of engineering and applied computer science, and engineering practitioners [2]. Zhou and Tang designed a complete and practical RSA encoding solution and provided analysis on the source codes based on NET platform [3]. Chaudhury et al. use asymmetric key based cryptographic algorithm using four prime numbers called ACAFP to handle four prime numbers and provide security [4]. Ashok Kumar Yadav discussed the blockchain basics overview, architecture, and blockchain security components such as hash function, Merkle tree, digital signature, and Elliptic curve cryptography (ECC) [5]. Lavanya K. Galla, et al. discuss the Public-key cryptosystems and the implementation of RSA algorithm in detail and the use of RSA in current software [6]. Osama Fouad et al. reduce the physical space on the various storage media and reduce the time of sending data over the Internet with a complete guarantee of encrypting this data and hiding it from intruders [7]. Das et al. elaborates a new asymmetric cryptography approach, i.e. modified RSA algorithm. This proposed method reduces complex calculation involved in RSA algorithm [8]. Amalarethinam and Leena's proposed algorithm reduces the time of encryption and decryption processes by dividing the file into blocks and enhances the strength of the algorithm by increasing the key size [9]. Nagar and Alshamma aim to speed up the implementation of the RSA algorithm during data transmission between different communication networks and Internet [10]. Soni and Rasool illustrate the algorithms along with flowcharts and implements, Trial Division, Quadratic Sieve Algorithm and Shor's Algorithm for factoring integers and lastly concludes with the observed facts and analyzed results [11]. Dhakar, Gupta and Sharma present a new cryptography algorithm based on additive homomorphic properties called Modified RSA Encryption Algorithm (MREA) [12]. Imam et al. compare RSA methods based on parameters such as key generation, encryption schemes, decryption schemes, key features and enhancements, and find the leading areas where modified RSA has been applied in the recent past [13]. Merkepci and Sarkis present a direct application for Pythagorean circles in the theory of cryptography by using integer points on these circles, as well as describing some numerical systems to generalize classical well-known crypto-algorithms and systems [14]. Jaju and Chowhan present a balanced comparison between the RSA and Modified RSA algorithms, evaluating both time and security aspects by conducting multiple encryption and decryption experiments using datasets of varying types [15].

However, with the advancement of quantum computers, the adequacy of classical encryption methods is being questioned, and the need for more resilient systems is increasing. Within this context, academic studies have increasingly focused on constructing more secure structures by increasing the complexity of RSA-like algorithms using extended number systems such as neutrosophic and plithogenic numbers.

The concept of plithogenic numbers has been introduced by Florentin Smarandache as an extended, multidimensional, and multi-attribute version of fuzzy, intuitionistic fuzzy, and neutrosophic systems. Unlike classical or fuzzy numbers, plithogenic numbers are defined not solely based on a single attribute or evaluation but rather through multiple attributes, criteria, and the interrelations among them. In a plithogenic system, there are multiple criteria (attributes), each associated with its own value, degree, and sometimes a degree of contradiction. When these values are combined, the resulting number or set acquires a multidimensional and significantly more complex structure.

A plithogenic set is defined as a set whose elements are characterized by one or more attributes, each of which can take multiple distinct values. For a given attribute value v, the degree of appurtenance of an element x to a plithogenic set P is denoted by d(x,v), In order to obtain more accurate results in plithogenic aggregation operations, a degree of contradiction or dissimilarity is defined between each attribute value and the dominant attribute value. Plithogenic aggregation operations include intersection, union, complement, inclusion, and equality. These operations depend on the degrees of contradiction between attribute values. Among them, the intersection and union operators are formulated as linear combinations of the t-norm and t-conorm operators used in fuzzy set theory.The plithogenic set constitutes a broader framework that generalizes classical, fuzzy, intuitionistic fuzzy, and neutrosophic sets. This is because these four types of sets are classified based on membership degrees: classical and fuzzy sets consider a single membership value; intuitionistic fuzzy sets involve both membership and non-membership values; and neutrosophic sets incorporate membership, non-membership, and indeterminacy values.

In recent years, plithogenic structures have become widely used in fields such as multi-criteria decision-making, artificial intelligence and machine learning, uncertainty-based systems, cryptography, and complex data analysis in medicine, engineering, and social sciences. As a result, the algebraic properties of plithogenic numbers have been investigated, and various researchers have contributed to this area. The foundational work in this field was carried out by Florentin Smarandache [16-18]. Subsequently, H. Merkepçi and M. Abobala introduced the algebraic properties of symbolic 2-plithogenic rings [19], while the

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2025.3620040

theory of symbolic 2-plithogenic numbers has further developed by H. Merkepçi and A. Rawashdeh [20]. Albasheer et Al. define and study the concept of symbolic 3-plithogenic rings asa novel extension of classical rings and symbolic 2-plithogenic rings respectively. Also, many related substructures will be presented such as idempotent elements, AH-ideals, AHS-homomorphisms, and kernels [21]. Rawashdeh gives the foundations number theory in 3-plithogenic rings of integers such as symbolic 3-plithogenic congruencies, division, and greatest common divisors [22]. R.Ali and Z.Hasan define the concept of symbolic 3-plithogenic modules based on symbolic 3-plithogenic sets and classical modules. Also, many related substructures will be defined and handled such as AH-functions, AH-submodules, and symbolic 3-plithogenic homomorphisms [23]. Alhasan presents the extended study of the 2-symbolic plithogenic numbers, where he studies the square root of a 2-symbolic plithogenic real number and 2-symbolic plithogenic real polynomial [24]. Basheer et al. define and study the concept of symbolic 3-plithogenic rings [25]. Von Shtawzen et al. presents the expansion of symbolic 2-plithogenic and symbolic 3-plithogenic real functions in one variable with real series [26]. H. Merkepçi finds easy-to-use algorithms for calculating the determinant of a symbolic 3-plithogenic and 4-plithogenic matrix, for finding its inverse based on its classical components, and even for diagonalizing matrices of these types [27].

This study aims to introduce a new dimension and perspective to the RSA algorithm in cryptology. By utilizing symbolic 2-plithogenic numbers, which incorporate two symbolic components, the objective is to enhance both the reliability and computational complexity of the encryption and decryption processes. To make the system even more secure and complex, the study further extends the approach by incorporating symbolic 3-plithogenic numbers, which are developed by extending symbolic 2-plithogenic numbers. With the inclusion of three symbolic components instead of two, the algorithm becomes significantly stronger, making decryption virtually impossible in unauthorized hands. The operations defined over these numbers such as addition, multiplication, and modular arithmetic are inherently more complex than their counterparts over classical integers. When integrated into cryptographic algorithms, particularly within frameworks like RSA, the integer factorization problem transforms into a multidimensional challenge. These number systems can be employed in the development of extended versions of classical encryption algorithms such as RSA. In such systems, an attacker must solve the entire multidimensional structure rather than isolating and targeting a single component, which considerably increases the complexity of brute-force attacks. As a result, it becomes feasible to construct encryption schemes that are more resistant to quantum computer-based attacks.

II. Preliminaries

In this section, we give some basic definitions and theorems that will make our work easier to understand.

Definition 2.1 [15] RSA algorithm is given as follows.

Key Generation

1. Choose two large distinct prime numbers p and q ($p \neq q$).

2. Compute $n = p \times q$.

3. Compute Euler's totient function $\varphi(n) = (p - 1) \times (q - 1)$.

4. Choose a public exponent e such that:

   $1 < e < \varphi(n)$

   $\gcd(e, \varphi(n)) = 1$

5. Compute the private exponent d such that:

   $d \equiv e^{-1} \pmod{\varphi(n)}$

6. The public key is (e, n)

7. The private key is (d, n)

Encryption

1. Convert plain text M into an integer such that $0 \leq M < n$.

2. Compute the ciphertext:

   $C = M^e \bmod n$

Decryption

1. Compute the plaintext:

   $M = C^d \bmod n$

Definition 2.2. [19] Let Rbe a ring. The corresponding symbolic 2-plithogenic ring is defined as follows:

$$2 - SP_R = \{m_0 + m_1P_1 + m_2P_2 : m_i \in R, P_j^2 = P_j, P_i.P_j = P_{\max(i,j)}\}$$

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2025.3620040

Definition 2.3. [20] Let $R = \mathbb{Z}$ be the ring of integers. The corresponding symbolic 2- plithogenic ring is

called $2 - SP_{\mathbb{Z}}$. $M = m_0 + \sum_{i=1}^{2} m_i P_i \in 2 - SP_{\mathbb{Z}}$ is positive symbolic 2-plithogenic integer if

$$m_0 > 0,$$

$$m_0 + m_1 > 0,$$

$$m_0 + m_1 + m_2 > 0.$$

Definition 2.4. [20] Let $M = m_0 + \sum_{i=1}^{2} m_i P_i$ and $N = n_0 + \sum_{i=1}^{2} n_i P_i$be elements of $2 - SP_{\mathbb{Z}}$. We say that $M \leq N$ if

$$m_0 \leq n_0,$$

$$m_0 + m_1 \leq n_0 + n_1,$$

$$m_0 + m_1 + m_2 \leq n_0 + n_1 + n_2.$$

Theorem 2.1. [20] Let $M = m_0 + \sum_{i=1}^{2} m_i P_i$ and $N = n_0 + \sum_{i=1}^{2} n_i P_i \in 2 - SP_{\mathbb{Z}}$. Then, $gcd(M, N) = 1$ if and only if

$$gcd(m_0, n_0) = 1,$$

$$gcd(m_0 + m_1, n_0 + n_1) = 1,$$

$$gcd(m_0 + m_1 + m_2, n_0 + n_1 + n_2) = 1,$$

if $gcd(M, N) = 1$, then,

$$\begin{aligned} M^{-1}(mod\, N) = {} & {m_0}^{-1}(mod\, n_0) \\ & + P_1[(m_0 + m_1)^{-1}(mod\, n_0 + n_1) \\ & - m_0^{-1}(mod\, n_0)] \\ & + P_2[(m_0 + m_1 + m_2)^{-1}(mod\, n_0 + n_1 + n_2) \\ & - (m_0 + m_1)^{-1}(mod\, n_0 + n_1)] \end{aligned}$$

Definition 2.5. [20] Let $M = m_0 + \sum_{i=1}^{2} m_i P_i > 0$ be a symbolic 2-plithogenic integer.

Define $\varphi_S: 2 - SP_{\mathbb{Z}} \to 2 - SP_{\mathbb{Z}}$ such that

$$\begin{aligned} \varphi_S(M) = {} & \varphi_S(m_0 + m_1 P_1 + m_2 P_2) \\ = {} & \varphi(m_0) + P_1[\varphi(m_0 + m_1) - \varphi(m_0)] \\ & + P_2[\varphi(m_0 + m_1 + m_2) - \varphi(m_0 + m_1)] \end{aligned}$$

where $\varphi$is the classical Phi-Euler's function.

Theorem 2.2. [20] Let $M = m_0 + \sum_{i=1}^{2} m_i P_i$, $N = n_0 + \sum_{i=1}^{2} n_i P_i \in 2 - SP_{\mathbb{Z}}$ and $gcd(M, N) = 1$, then

$M^{\varphi_S(N)} \equiv 1(mod\, N)$.

Definition 2.6. [21] Let R be a ring. The corresponding symbolic 3-plithogenic ring is defined as follows:

$$\begin{aligned} 3 - SP_R = \{ & e_0 + e_1 P_1 + e_1 P_1 + e_2 P_2 + e_3 P_3 : e_i \in \\ & R,\ P_j^2 = P_j,\ P_i P_j = P_{max(i,j)} \} \end{aligned}$$

Definition 2.7. [22] Let $R = \mathbb{Z}$ be the ring of integers. The corresponding symbolic 3-plithogenic ring is called $3 - SP_{\mathbb{Z}}$. $E = e_0 + \sum_{i=1}^{3} e_i P_i \in 3 - SP_{\mathbb{Z}}$ is positive symbolic 3-plithogenic integer if

$$e_0 > 0,$$

$$e_0 + e_1 > 0,$$

$$e_0 + e_1 + e_2 > 0,$$

$$e_0 + e_1 + e_2 + e_3 > 0\ .$$

Definition 2.8. [22] Let $E = e_0 + \sum_{i=1}^{3} e_i P_i$ and $F = f_0 + \sum_{i=1}^{3} f_i P_i \in 3 - SP_{\mathbb{Z}}$. Then $gcd(E, F) = 1$ if and only if

$$gcd(e_0, f_0) = 1,$$

$$gcd(e_0 + e_1, f_0 + f_1) = 1,$$

$$gcd(e_0 + e_1 + e_2, f_0 + f_1 + f_2) = 1,$$

$$gcd(e_0 + e_1 + e_2 + e_3, f_0 + f_1 + f_2 + f_3) = 1.$$

if $gcd(E, F) = 1$, then,

$$\begin{aligned} E^{-1}(mod\, F) = {} & e_0^{-1}(mod\, f_0) \\ & + P_1[(e_0 + e_1)^{-1}(mod\, f_0 + f_1) \\ & - e_0^{-1}(mod\, f_0)] \\ & + P_2[(e_0 + e_1 + e_2)^{-1}(mod\, f_0 + f_1 + f_2) \\ & - (e_0 + e_1)^{-1}(mod\, f_0 + f_1)] \\ & + P_3[(e_0 + e_1 + e_2 + e_3)^{-1}(mod\, f_0 + f_1 + f_2 + f_3) \\ & - (e_0 + e_1 + e_2)^{-1}(mod\, f_0 + f_1 + f_2)] \end{aligned}$$

Definition 2.9. [22] Let $E = e_0 + \sum_{i=1}^{3} e_i P_i > 0$ be a symbolic 3-plithogenic integer, define

$\varphi_S: 3 - SP_{\mathbb{Z}} \to 3 - SP_{\mathbb{Z}}$ such that

$$\begin{aligned} \varphi_S(E) = {} & \varphi(e_0) + P_1[\varphi(e_0 + e_1) - \varphi(e_0)] \\ & + P_2[\varphi(e_0 + e_1 + e_2) - \varphi(e_0 + e_1)] \\ & + P_3[\varphi(e_0 + e_1 + e_2 + e_3) - \varphi(e_0 + e_1 + e_2)] \end{aligned}$$

where $\varphi$is the classical Phi-Euler's function.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2025.3620040

Theorem 2.3. [22] Let $E = e_0 + \sum_{i=1}^{3} e_i P_i$,

$F = f_0 + \sum_{i=1}^{3} f_i P_i \in 3 - SP_{\mathbb{Z}}$ and

$gcd(E, F) = 1$, then , $E^{\varphi_S(F)} \equiv 1 (mod\, F)$.

III. Methodology

In this article, we recommend an asymmetric key based on RSA algorithm using symbolic 2-plithogenic and 3-plithogenic numbers. This method is split into three parts such as key generation, encryption, decryption. Figure 1 presents a general overview of the system. Let's explain the algorithm steps for symbolic 2-plithogenic and 3-plithogenic numbers, respectively.

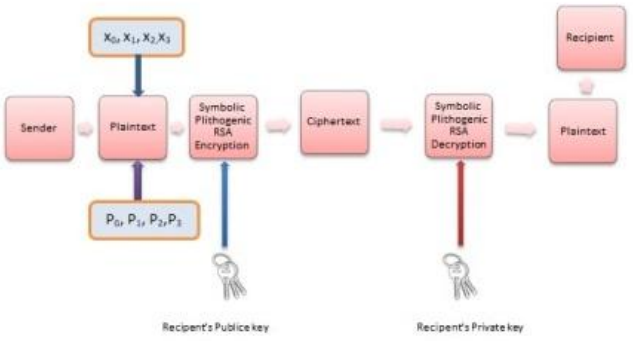

Figure 1. General overwiew of the system

Symbolic 2-Plithogenic Algorithms

Algorithm 1: Symbolic 2-Plithogenic Key Generation

1. Let $X = x_0 + x_1 P_1 + x_2 P_2$,

$Y = y_0 + y_1 P_1 + y_2 P_2$ be two positive symbolic 2-plithogenic integers satisfying these conditions: $x_0 > 0$,

$$x_0 + x_1 > 0,$$

$$x_0 + x_1 + x_2 > 0$$

and $y_0 > 0$,

$$y_0 + y_1 > 0,$$

$$y_0 + y_1 + y_2 > 0.$$

Additionally, x_0, y_0, $x_0 + x_1$,$y_0 + y_1$, $x_0 + x_1 + x_2$, $y_0 + y_1 + y_2$ are randomly large primes such that $gcd(x_0, y_0) = 1$, $gcd(x_0 + x_1, y_0 + y_1) = 1$,

$gcd(x_0 + x_1 + x_2, y_0 + y_1 + y_2) = 1$.

2. Compute $N = X.Y$

$$\begin{aligned} N &= (x_0 + x_1 P_1 + x_2 P_2)(y_0 + y_1 P_1 + y_2 P_2) \\ &= x_0 y_0 + P_1(x_0 y_1 + x_1 y_0 + x_1 y_1) \\ &\quad + P_2(x_0 y_2 + x_2 y_0 + x_1 y_2 \\ &\quad + x_2 y_1 + x_2 y_2) \\ &= n_0 + n_1 P_1 + n_2 P_2. \end{aligned}$$

where,

$$x_0 y_0 = n_0,$$

$$x_0 y_1 + x_1 y_0 + x_1 y_1 = n_1,$$

$$x_0 y_2 + x_2 y_0 + x_1 y_2 + x_2 y_1 + x_2 y_2 = n_2.$$

3. A specially defined function

$\varphi_S: 2 - SP_Z \to 2 - SP_Z$ is used to compute $\varphi_S(N)$ via the symbolic Phi-Euler's function such that

$$\begin{aligned} \varphi_S(N) &= \varphi(n_0) + P_1[\varphi(n_0 + n_1) - \varphi(n_0)] \\ &\quad + P_2[\varphi(n_0 + n_1 + n_2) \\ &\quad - \varphi(n_0 + n_1)] \\ &= t_0 + t_1 P_1 + t_2 P_2 \end{aligned}$$

where,

$$\varphi(n_0) = t_0,$$

$$\varphi(n_0 + n_1) - \varphi(n_0) = t_1,$$

$$\varphi(n_0 + n_1 + n_2) - \varphi(n_0 + n_1) = t_2$$

or ıt can be found as follows:

$$\begin{aligned} \varphi_S(N) &= (X - 1).(Y - 1) \\ &= \big((x_0 - 1) + x_1 P_1 + x_2 P_2\big)\big((y_0 - 1) \\ &\quad + y_1 P_1 + y_2 P_2\big) \end{aligned}$$

4. Now, select a positive symbolic 2-plithogenic integer $E = e_0 + e_1 P_1 + e_2 P_2 > 0$ such that

$1 < E < \varphi_S(N)$ and $gcd\big(E, \varphi_S(N)\big) = 1$. Namely,

$1 < e_0 < t_0$, $\quad \gcd(e_0, t_0) = 1$

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2025.3620040

$1 < e_0 + e_1 < t_0 + t_1 \ \gcd(e_0 + e_1, t_0 + t_1) = 1$
$1 < e_0 + e_1 + e_2 < t_0 + t_1 + t_2,$

$$\gcd(e_0 + e_1 + e_2, t_0 + t_1 + t_2) = 1$$

The value of E determined under these conditions, thus, the public key is generated and given by the pair (E, N).

Algorithm 2. Symbolic 2-Plithogenic Encryption

1. Let $M = m_0 + m_1P_1 + m_2P_2 \in 2 - SP_Z$ be plaintext to be encrypted using the public key (E, N). The ciphertext is denoted by C.
2. $C \equiv M^E (mod\ N)$.
3. $M^E (mod\ N) = (m_0 + m_1P_1 + m_2P_2)^{e_0+e_1P_1+e_2P_2} (mod\ n_0 + n_1P_1 + n_2P_2)$
$= {m_0}^{e_0} (mod\ n_0) + P_1[(m_0 + m_1)^{e_0+e_1} (mod\ n_0 + n_1) - {m_0}^{e_0} (mod\ n_0)]$
$+P_2[(m_0 + m_1 + m_2)^{e_0+e_1+e_2} (mod\ n_0 + n_1 + n_2) - (m_0 + m_1)^{e_0+e_1} (mod\ n_0 + n_1)]$
$= c_0 + c_1P_1 + c_2P_2.$

Algorithm 3: Symbolic 2-Plithogenic Decryption

1. The ciphertext is $C \equiv M^E (mod\ N)$, thus situated the plaintext $M \equiv C^{E^{-1}} (mod\ N)$.
2. $E^{-1} = {e_0}^{-1} (mod\ t_0) + P_1[(e_0 + e_1)^{-1} (mod\ t_0 + t_1) - {e_0}^{-1} (mod\ t_0)]$
$+P_2[(e_0 + e_1 + e_2)^{-1} (mod\ t_0 + t_1 + t_2) - (e_0 + e_1)^{-1} (mod\ t_0 + t_1)]$
$= d_0 + d_1P_1 + d_2P_2 = D$

   So, the private key is generated and given by the pair (D, N).

3. $M \equiv C^D (mod\ N)$
$= {c_0}^{d_0} (mod\ n_0) + P_1[(c_0 + c_1)^{d_0+d_1} (mod\ n_0 + n_1) - {c_0}^{d_0} (mod\ n_0)]$
$+P_2[(c_0 + c_1 + c_2)^{d_0+d_1+d_2} (mod\ n_0 + n_1 + n_2) - (c_0 + c_1)^{d_0+d_1} (mod\ n_0 + n_1)].$

Symbolic 3-Plithogenic Algorithms

Algorithm 1: Symbolic 3-Plithogenic Key Generation

1. Let $X = x_0 + x_1P_1 + x_2P_2 + x_3P_3,$

$Y = y_0 + y_1P_1 + y_2P_2 + y_3P_3$ be two positive symbolic 3-plithogenic integers satisfying these conditions:

$$x_0 > 0,$$

$$x_0 + x_1 > 0,$$

$$x_0 + x_1 + x_2 > 0\ ,$$

$$x_0 + x_1 + x_2 + x_3 > 0$$

and

$$y_0 > 0,$$

$$y_0 + y_1 > 0,$$

$$y_0 + y_1 + y_2 > 0,$$

$$y_0 + y_1 + y_2 + y_3 > 0.$$

Additionally, x_0, y_0, $x_0 + x_1$,$y_0 + y_1$, $x_0 + x_1 + x_2$, $y_0 + y_1 + y_2$, $x_0 + x_1 + x_2 + x_3$,$y_0 + y_1 + y_2 + y_3$ are randomly large primes such that $gcd(x_0, y_0) = 1,$

$$gcd(x_0 + x_1, y_0 + y_1) = 1,$$

$$gcd(x_0 + x_1 + x_2, y_0 + y_1 + y_2) = 1,$$

$$gcd(x_0 + x_1 + x_2 + x_3, y_0 + y_1 + y_2 + y_3) = 1.$$

2. Compute $N = X.Y$

$N = (x_0 + x_1P_1 + x_2P_2 + x_3P_3)(y_0 + y_1P_1 + y_2P_2 + y_3P_3)$
$= x_0y_0 + P_1(x_0y_1 + x_1y_0 + x_1y_1) + P_2(x_0y_2 + x_2y_0 + x_1y_2 + x_2y_1 + x_2y_2)$
$+P_3[x_0y_3 + x_3y_0 + x_1y_3 + x_3y_1 + x_2y_3 + x_3y_2 + x_3y_3]$
$= n_0 + n_1P_1 + n_2P_2 + n_3P_3$

where,

$$x_0y_0 = n_0,$$

$$x_0y_1 + x_1y_0 + x_1y_1 = n_1,$$

$$x_0y_2 + x_2y_0 + x_1y_2 + x_2y_1 + x_2y_2 = n_2,$$

$$x_0y_3 + x_3y_0 + x_1y_3 + x_3y_1 + x_2y_3 + x_3y_2 + x_3y_3 = n_3.$$

3. A specially defined function

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2025.3620040

4. $\varphi_S: 3-SP_Z \to 3-SP_Z$ is used to compute $\varphi_S(N)$ via the symbolic Phi-Euler's function such that

$$\begin{aligned}\varphi_S(N) &= \varphi(n_0) + P_1[\varphi(n_0+n_1)-\varphi(n_0)] \\ &\quad + P_2[\varphi(n_0+n_1+n_2) \\ &\quad - \varphi(n_0+n_1)] \\ &+P_3[\varphi(n_0+n_1+n_2+n_3)-\varphi(n_0+n_1+n_2)] \\ &= t_0 + t_1P_1 + t_2P_2 + t_3P_3\end{aligned}$$

where,

$$\varphi(n_0) = t_0,$$

$$\varphi(n_0+n_1)-\varphi(n_0) = t_1,$$

$$\varphi(n_0+n_1+n_2)-\varphi(n_0+n_1) = t_2.$$

$$\varphi(n_0+n_1+n_2+n_3)-\varphi(n_0+n_1+n_2) = t_3$$

or ıt can be found as follows:

$$\begin{aligned}\varphi_S(N) &= (X-1).(Y-1) \\ &= \big((x_0-1)+x_1P_1+x_2P_2+x_3P_3\big)\big((y_0-1) \\ &\quad + y_1P_1+y_2P_2+y_3P_3\big)\end{aligned}$$

5. Now, select a positive symbolic 3-plithogenic integer $E = e_0 + e_1P_1 + e_2P_2 + e_3P_3 > 0$ such that

$1 < E < \varphi_S(N)$ and $gcd\big(E, \varphi_S(N)\big) = 1$. Namely,

$$1 < e_0 < t_0\,, \qquad \gcd(e_0, t_0) = 1$$

$$1 < e_0 + e_1 < t_0 + t_1,$$

$$\gcd(e_0+e_1, t_0+t_1) = 1$$

$$1 < e_0+e_1+e_2 < t_0+t_1+t_2,$$

$$\gcd(e_0+e_1+e_2, t_0+t_1+t_2) = 1$$

$$1 < e_0+e_1+e_2+e_3 < t_0+t_1+t_2+t_3,$$

$$\gcd(e_0+e_1+e_2+e_3, t_0+t_1+t_2+t_3) = 1$$

The value of E determined under these conditions, thus, the public key is generated and given by the pair (E, N).

Algorithm 2. Symbolic 3-Plithogenic Encryption

1. Let $M = m_0 + m_1P_1 + m_2P_2 + m_3P_3 \in 3-SP_Z$ be plaintext to be encrypted using the public key (E, N). The ciphertext is denoted by C.
2. $C \equiv M^E (mod\ N)$.
3. $M^E (mod\ N) = (m_0 + m_1P_1 + m_2P_2 + m_3P_3)^{e_0+e_1P_1+e_2P_2+e_3P_3} (mod\ n_0 + n_1P_1 + n_2P_2 + n_3P_3)$

$$\begin{aligned}&= {m_0}^{e_0}(mod\ n_0) + P_1[(m_0+m_1)^{e_0+e_1}(mod\ n_0 \\ &\quad + n_1) - {m_0}^{e_0}(mod\ n_0)] \\ &+P_2[(m_0+m_1+m_2)^{e_0+e_1+e_2}(mod\ n_0+n_1 \\ &\quad + n_2) \\ &\quad - (m_0+m_1)^{e_0+e_1}(mod\ n_0 \\ &\quad + n_1)] \\ &+P_3[(m_0+m_1+m_2+m_3)^{e_0+e_1+e_2+e_3}(mod\ n_0 \\ &\quad + n_1+n_2+n_3) \\ &\quad - (m_0+m_1 \\ &\quad + m_2)^{e_0+e_1+e_2}(mod\ n_0+n_1 \\ &\quad + n_2)] \\ &= c_0 + c_1P_1 + c_2P_2 + c_3P_3\end{aligned}$$

Algorithm 3: Symbolic 3-Plithogenic Decryption

1. The ciphertext is $C \equiv M^E (mod\ N)$, thus situated the plaintext $M \equiv C^{E^{-1}} (mod\ N)$.
2. $E^{-1} = {e_0}^{-1}(mod\ t_0) + P_1[(e_0+e_1)^{-1}(mod\ t_0 + t_1) - {e_0}^{-1}(mod\ t_0)]$

$$\begin{aligned}&+P_2[(e_0+e_1+e_2)^{-1}(mod\ t_0+t_1+t_2) \\ &\quad - (e_0+e_1)^{-1}(mod\ t_0+t_1)] \\ &+P_3[(e_0+e_1+e_2+e_3)^{-1}(mod\ t_0+t_1+t_2 \\ &\quad + t_3) \\ &\quad - (e_0+e_1+e_2)^{-1}(mod\ t_0+t_1 \\ &\quad + t_2)] \\ &= d_0 + d_1P_1 + d_2P_2 + d_3P_3 = D\end{aligned}$$

So, the private key is generated and given by the pair (D, N).

$$\begin{aligned}&\boldsymbol{M \equiv C^D (mod\ N)} \\ &\boldsymbol{= {c_0}^{d_0}(mod\ n_0) + P_1\big[(c_0+c_1)^{d_0+d_1}(mod\ n_0} \\ &\quad \boldsymbol{+ n_1) - {c_0}^{d_0}(mod\ n_0)\big]} \\ &\boldsymbol{+P_2\big[(c_0+c_1+c_2)^{d_0+d_1+d_2}(mod\ n_0+n_1+n_2)} \\ &\quad \boldsymbol{- (c_0+c_1)^{d_0+d_1}(mod\ n_0+n_1)\big]} \\ &\boldsymbol{+P_3\big[(c_0+c_1+c_2+c_3)^{d_0+d_1+d_2+d_3}(mod\ n_0+n_1} \\ &\quad \boldsymbol{+ n_2+n_3)} \\ &\quad \boldsymbol{- (c_0+c_1+c_2)^{d_0+d_1+d_2}(mod\ n_0} \\ &\quad \boldsymbol{+ n_1+n_2)\big]}\end{aligned}$$

IV. NUMERIC EXAMPLES

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2025.3620040

The methodology can be generated using a MATLAB program. This allows for the creation of thousands or even hundreds of thousands of combinations. As an example, we selected a symbolic 2-plithogenic number composed of large prime numbers.

Example 4.1. In this example, we give the encryption of a message M that we choose from symbolic 2 plithogenic numbers. So, we select Symbolic 2-Plithogenic numbers compose of large prime numbers.

Algorithm 1: Symbolic 2-Plithogenic Key Generation

1. Let $X = 47 + 12P_1 - 48P_2$, $Y = 41 - 18P_1 - 4P_2$be two positive symbolic 2-plithogenic integers

satisfying these conditions: $47 > 0, 59 > 0, 11 > 0$ and $41 > 0, 23 > 0, 19 > 0$. Additionally, 47, 41, 59,23, 11, 19 are randomly large primes such that $gcd(47,41) = 1$, $gcd(59,23) = 1$, $gcd(11,19) = 1$.

2. Compute $N = X.Y$

$$N = (47 + 12P_1 - 48P_2)(41 - 18P_1 - 4P_2)$$
$$= 1927 + P_1(-846 + 492 - 216) + P_2(-188 - 48 - 1968 + 864 + 192)$$
$$= 1927 - 570P_1 - 1148P_2$$

where, $1927 = n_0$, $-570 = n_1$, $-1148 = n_2$.

3. A specially defined function $\varphi_S: 2 - SP_Z \to 2 - SP_Z$ is used to compute $\varphi_S(N)$ via the symbolic Phi-Euler's function such that

$$\varphi_S(N) = \varphi(1927) + P_1[\varphi(1357) - \varphi(1927)] + P_2[\varphi(209) - \varphi(1357)]$$
$$= 1840 - 564P_1 - 1096P_2$$

where, $1840 = t_0$, $-564 = t_1$, $-1096 = t_2$.

4. Now, select a positive symbolic 2-plithogenic integer $E = e_0 + e_1P_1 + e_2P_2 > 0$ such that

$1 < E < \varphi_S(N)$ and $gcd(E, \varphi_S(N)) = 1$. Namely,

$1 < 89 < 1840$, $\gcd(89,1840) = 1$
$1 < 97 < 1276$, $\gcd(97,1276) = 1$
$1 < 103 < 180$, $\gcd(103,180) = 1$

So, $e_0 = 89$, $e_1 = 8$, $e_2 = 6$ and $E = 89 + 8P_1 + 6P_2$.

The value of Edetermined under these conditions, thus, the public key is generated and given by the pair (E, N).

Algorithm 2. Symbolic 2-Plithogenic Encryption

1. Let $M = 35 + 45P_1 + 57P_2 \in 2 - SP_Z$be plaintext to be encrypted using the public key (E, N). The ciphertext is denoted by C.

2. $C \equiv M^E (mod\, N)$.

3. $M^E (mod\, N) = (35 + 45P_1 + 57P_2)^{89+8P_1+6P_2} (mod\, 1\,927 - 570P_1 - 1148P_2)$
$C = 35^{89} (mod\, 1\,927) + P_1[(80)^{97} (mod\, 1\,357) - 35^{89} (mod\, 1\,927)]$
$+P_2[(137)^{103} (mod\, 2\,09) - (80)^{97} (mod\, 1\,357)]$
$C = 1252 + P_1(1307 - 1252) + P_2(180 - 1307)$
$C = 1252 + 55P_1 - 1127P_2$.

Algorithm 3: Symbolic 2-Plithogenic Decryption

1. The ciphertext is $C \equiv M^E (mod\, N)$, thus situated the plaintext $M \equiv C^{E^{-1}} (mod\, N)$.

2.$E^{-1} = 89^{-1} (mod\, 1\,840) + P_1[(97)^{-1} (mod\, 1\,276) - 89^{-1} (mod\, 1\,840)]$
$+P_2[(103)^{-1} (mod\, 1\,80) - (97)^{-1} (mod\, 1\,276)]$
$= 889 + P_1(1105 - 889) + P_2(7 - 1105)$
$E^{-1} = D = 889 + 216P_1 - 1098P_2$

So, the private key is generated and given by the pair (D, N).

3. $M \equiv C^D (mod\, N)$
$= 1252^{889} (mod\, 1\,927) + P_1[(1307)^{1105} (mod\, 1\,357) - 1252^{889} (mod\, 1\,927)]$
$+P_2[(180)^7 (mod\, 2\,09) - (1307)^{1105} (mod\, 1\,357)]$
$M = 35 + P_1(80 - 35) + P_2(137 - 80)$
$M = 35 + 45P_1 + 57P_2$.

Example 4.2. In this example, we give the encryption of a message M that we choose from symbolic 3 plithogenic numbers. So, we select Symbolic 3-Plithogenic numbers compose of large prime numbers.

Algorithm 1: Symbolic 3-Plithogenic Key Generation

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2025.3620040

1. Let $X = 73 + 54P_1 + 52P_2 + 72P_3$, $Y = 67 + 64P_1 + 50P_2 + 52P_3$be two positive symbolic 3-plithogenic integers satisfying these conditions: $73 > 0$, $127 > 0$, $179 > 0$, $251 > 0$ and $67 > 0$, $131 > 0$, $181 > 0$ $233 > 0$. Additionally, 73, 67, 127,131, 179, 181, 251,233 are randomly large primes such that $gcd(73,67) = 1$, $gcd(127,131) = 1$, $gcd(179,181) = 1$, $gcd(251,233) = 1$.
2. Compute $N = X.Y$

$$N = (73 + 54P_1 + 52P_2 + 72P_3)(67 + 64P_1 + 50P_2 + 52P_3)$$
$$= 4891 + P_1(4672 + 3618 + 3456) + P_2(3650 + 2700 + 3484 + 3328 + 2600) + P_3(3796 + 2808 + 2704 + 4824 + 4608 + 3600 + 3744)$$
$$N = 4891 + 11746P_1 + 15762P_2 + 26084P_3$$

where, $4891 = n_0$, $11746 = n_1$, $15762 = n_2$,$26084 = n_3$.

3. A specially defined function $\varphi_S: 3 - SP_Z \to 3 - SP_Z$ is used to compute $\varphi_S(N)$ via the symbolic Phi-Euler's function such that

$$\varphi_S(N) = (72 + 54P_1 + 52P_2 + 72P_3)(66 + 64P_1 + 50P_2 + 52P_3)$$
$$= 4752 + P_1(4608 + 3564 + 3456) + P_2(3600 + 2700 + 3432 + 3328 + 2600) + P_3(3744 + 2808 + 2704 + 4752 + 4608 + 3600 + 3744)$$
$$\varphi_S(N) = 4752 + 11628P_1 + 15660P_2 + 25960P_3$$

where, $4752 = t_0$, $11628 = t_1$, $15660 = t_2$,$25960 = t_3$.

4. Now, select a positive symbolic 3-plithogenic integer $E = e_0 + e_1P_1 + e_2P_2 + e_3P_3 > 0$ such that $1 < E < \varphi_S(N)$ and $gcd\big(E, \varphi_S(N)\big) = 1$. Namely,

$1 < 611 < 4752$, $\gcd(611,4752) = 1$
$1 < 899 < 16380$, $\gcd(899,16380) = 1$

$1 < 1291 < 32040$,

$\gcd(1291,32040) = 1$

$1 < 2727 < 58000$,

$\gcd(2727,58000) = 1$

So, $e_0 = 611$, $e_1 = 288$, $e_2 = 392$, $e_3 = 1436$ and $E = 611 + 288P_1 + 392P_2 + 1436P_3$.

The value of Edetermined under these conditions, thus, the public key is generated and given by the pair (E, N).

Algorithm 2. Symbolic 3-Plithogenic Encryption

1. Let $M = 2257 + 1237P_1 + 2300P_2 + 1436P_3 \in 3 - SP_Z$be plaintext to be encrypted using the public key (E, N). The ciphertext is denoted by C.
2. $C \equiv M^E (mod\ N)$.
3. $C = (2257 + 1237P_1 + 2300P_2 + 1436P_3)^{611+288P_1+392P_2+1436P_3} (mod\ 4\,891 + 11746P_1 + 15762P_2 + 26084P_3)$
$= 2257^{611}(mod\ 4\,891) + P_1[3494^{899}(mod\ 1\,6637) - 2257^{611}(mod\ 4\,891)] + P_2[5794^{1291}(mod\ 3\,2399) - 3494^{899}(mod\ 1\,6637)] + P_3[7230^{2727}(mod\ 5\,8483) - 5794^{1291}(mod\ 3\,2399)]$
$C = 3735 - 327P_1 + 6826P_2 - 9309P_3$

Algorithm 3: Symbolic 3-Plithogenic Decryption

1. The ciphertext is $C \equiv M^E (mod\ N)$, thus situated the plaintext $M \equiv C^{E^{-1}} (mod\ N)$.
2. $E^{-1} = 611^{-1}(mod\ 4\,752) + P_1[899^{-1}(mod\ 1\,6380) - 611^{-1}(mod\ 4\,752)] + P_2[1291^{-1}(mod\ 3\,2040) - 899^{-1}(mod\ 1\,6380)] + P_3[2727^{-1}(mod\ 5\,8000) - 1291^{-1}(mod\ 3\,2040)]$
$E^{-1} = 2411 + P_1(13319 - 2411) + P_2(10771 - 13319) + P_3(48663 - 10771)$
$= 2411 + 10908P_1 - 2548P_2 + 37892P_3 = D$

So, the private key is generated and given by the pair (D, N).

$$M \equiv C^D (mod\ N)$$
$$= 3735^{2411}(mod\ 4\,891) + P_1[3408^{13319}(mod\ 1\,6637) - 3735^{2411}(mod\ 4\,891)] + P_2[10234^{10771}(mod\ 3\,2399) - 3408^{13319}(mod\ 1\,6637)] + P_3[925^{48663}(mod\ 5\,8483) - 10234^{10771}(mod\ 3\,2399)]$$
$$M = 2257 + P_1(3494 - 2257) + P_2(5794 - 3494) + P_3(7230 - 5794)$$

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2025.3620040

$$M = 2257 + 1237P_1 + 2300P_2 + 1436P_3.$$

V. DISCUSSION

The RSA algorithm is based on classical one-dimensional number systems for data encryption and decryption. Today, to enhance data confidentiality and reliability, algorithms built using number systems with three or more components offer increased security and trustworthiness. In this context, algorithms developed using neutrosophic number systems, which are three-dimensional, have been introduced. Plithogenic numbers are an extended form of neutrosophic numbers, containing four or more components. Encryption and decryption algorithms based on these number systems provide greater confidentiality and reliability. Table 1 below presents a comparison of the number systems.

TABLE I
COMPARISON OF NUMBER SYSTEMS IN ENCRYPTION

Feature	Classical RSA	Neutrosophic RSA	Plithogenic RSA
Number System	One-dimensional (integers, prime numbers)	3-component number system (truth, falsehood, indeterminacy)	4+ component advanced number system (complex contradictions, uncertainties, neutrality, etc.)
Mathematical Structure	Modular arithmetic, prime factorization	Neutrosophic logic, extended fuzzy set arithmetic	Plithogenic logic, multi-dimensional truth evaluation functions
Uncertainty Representation	None (fixed, definite numbers)	Present (can represent uncertainty and contradiction)	Higher-level uncertainty and dynamic representations
Security Level	Traditional security (based on factoring difficulty)	Additional security from uncertainty modeling	Enhanced security with multi-dimensional uncertainty
Encryption Application	Fixed and precise encryption-decryption operations	Variable structures, fuzzy encryption	Multi-component key structures with dynamic encryption
Use Cases	General digital communication, data security	Systems involving uncertainty (e.g., fuzzy data protection)	Artificial intelligence, multi-variable data systems, high-security environments

VI. CONCLUSION

The multidimensional nature of plithogenic structures ensures that keys depend not only on numerical magnitude but also on the symbolic properties of their components. In particular, the process of prime factorization becomes more challenging within multidimensional structures, thereby enhancing security. This leads to the creation of richer and more flexible key spaces compared to traditional RSA. While the use of symbolic plithogenic numbers in the RSA algorithm offers enhanced security and flexibility beyond conventional methods, it remains largely theoretical due to

current implementation challenges and performance limitations. This study especially contributes to the theoretical knowledge. The use of 2- and 3-plithogenic structures to increase algebraic complexity is theoretically intriguing and could open new directions in the development of post-quantum secure schemes.

REFERENCES

[1] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-keycryptosystems. Communications of the ACM, 21(2), 120–126. https://doi.org/10.1145/359340.359342
[2] Paar, C., & Pelzl, J. (2009). Understanding Cryptography: A Textbook for Students and Practitioners. Springer.
[3] Zhou, Xin, and Xiaofei Tang. "Research and implementation of RSA algorithm for encryption and decryption." Proceedings of 2011 6th international forum on strategic technology. Vol. 2. IEEE, 2011.
[4] Chaudhury, Punit, et al. "ACAFP: Asymmetric key based cryptographic algorithm using four prime numbers to secure message communication. A review on RSA algorithm." 2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON). IEEE, 2017.
[5] Yadav, Ashok Kumar. "Significance of elliptic curve cryptography in blockchain IoT with comparative analysis of RSA algorithm." 2021 international conference on computing, communication, and intelligent systems (icccis). IEEE, 2021.
[6] Galla, Lavanya K., Venkata SreeKrishna Koganti, and Nagarjuna Nuthalapati. "Implementation of RSA." 2016 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT). IEEE, 2016.
[7] Osama Fouad et al. "Hiding data using efficient combination of RSA cryptography, and compression steganography techniques." IEEE access 9 (2021): 31805-31815.
[8] Das, Sudhansu & Mishra, Sugyan & Sahu, Anup. (2020). A New Modified Version of Standard RSA Cryptography Algorithm. 10.1007/978-981-13-9680-9_24.
[9] Amalarethinam, I. George, and H. M. Leena. "Enhanced RSA algorithm with varying key sizes for data security in cloud." 2017 World congress on computing and communication technologies (WCCCT). IEEE, 2017.
[10] Nagar, Sami A., and Saad Alshamma. "High speed implementation of RSA algorithm with modified keys exchange." 2012 6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT). IEEE, 2012.
[11] Soni, Kapil Kumar, and Akhtar Rasool. "Cryptographic attack possibilities over RSA algorithm through classical and quantum computation." 2018 International Conference on Smart Systems and Inventive Technology (ICSSIT). IEEE, 2018.
[12] R. S. Dhakar, A. K. Gupta and P. Sharma, "Modified RSA Encryption Algorithm (MREA)," 2012 Second International Conference on Advanced Computing & Communication Technologies, Rohtak, India, 2012, pp. 426-429, doi: 10.1109/ACCT.2012.74.
[13] R. Imam, Q. M. Areeb, A. Alturki and F. Anwer, "Systematic and Critical Review of RSA Based Public Key Cryptographic Schemes: Past and Present Status," in IEEE Access, vol. 9, pp. 155949-155976, 2021,
[14] Merkepci, M., Sarkis, M. An Application of Pythagorean Circles in Cryptography and Some Ideas for Future Non-Classical Systems. Galoitica Journal of Mathematical Structures and Applications 2022.
[15] S. A. Jaju and S. S. Chowhan, "A Modified RSA algorithm to enhance security for digital signature," 2015 International Conference and Workshop on Computing and Communication

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2025.3620040

(IEMCON), Vancouver, BC, Canada, 2015, pp. 1-5, doi: 10.1109/IEMCON.2015.7344493.
[16] F. Smarandache, Plithogeny, Plithogenic Set, Logic, Probability, and Statistics, 141 pages, Pons Editions,Brussels, Belgium, 2017. arXiv.org (Cornell University), Computer Science - Artificial Intelligence, 03Bxx:
[17] Florentin Smarandache: Plithogenic Set, an Extension of Crisp, Fuzzy, Intuitionistic Fuzzy, and Neutrosophic Sets – Revisited, Neutrosophic Sets and Systems, vol. 21, 2018, pp. 153-166.
[18] Smarandache, F., " Introduction to the Symbolic Plithogenic Algebraic Structures (revisited)", Neutrosophic Sets and Systems, vol. 53, pp.653-665, 2023.
[19] Merkepci, H. Abobala, M. "On the Symbolic 2-Plithogenic Rings," International Journal of Neutrosophic Science, vol. 20, no.3 , pp. 115-122, 2023. DOI: https://doi.org/10.54216/IJNS.200311
[20] Merkepci, H., and Rawashdeh, A., " On The Symbolic 2-Plithogenic Number Theory and Integers ", Neutrosophic Sets and Systems, Vol 54, pp. 113-123. 2023. DOI: 10.5281/zenodo.7817721
[21] Albasheer, O., Hajjari., A., and Dalla., R., " On The Symbolic 3-Plithogenic Rings and Their Algebraic Properties", Neutrosophic Sets and Systems, Vol 54, pp.57-67, 2023.
[22] Rawashdeh, A. (2023). An Introduction To The Symbolic 3-Plithogenic Number Theory. Neoma Journal of Mathematics and Computer Science, 1(1). https://doi.org/10.5281/zenodo.7955676
[23] Ali, R. Hasan, Z. "An Introduction To The Symbolic 3-Plithogenic Modules," Galoitica: Journal of Mathematical Structures and Applications, vol. 6, no.1, pp. 13-17, 2023. DOI: https://doi.org/10.54216/GJMSA.060102
[24] Alhasan, Yaser Ahmad. "The Extended Study of the 2-symbolic Plithogenic Numbers." Plithogenic Logic and Computation 2 (2024): 37-48.
[25] Basheer, Othman Al, Arwa Hajjari, and Rasha Dalla. "On the symbolic 3-plithogenic rings and their algebraic properties." Neutrosophic Sets and Systems Vol.54.1 (2023), pp.57-67.
[26] Von Shtawzen, Oliver, Bahadir Tantay, and Foziljonov Ibrohimjon. "On Some Symbolic 2-Plithogenic and 3-Plithogenic Real Series." International Journal of Neutrosophic Science (IJNS) 23.4, pp.292-301, (2024).
[27] Merkepçi, Hamiyet. "On novel results about the algebraic properties of symbolic 3-plithogenic and 4-plithogenic real square matrices." Symmetry 15.8 (2023): 1494.

MEHMET MERKEPÇI was born on January 1st, 1979 in Gaziantep, Türkiye. He received the B.Sc. degree in electrical electronics engineering from Karadeniz Technical University, Trabzon, Türkiye, M.Sc. degree in electrical electronics from Gaziantep University, Gaziantep, Türkiye and PhD. degree in electrical electronics from Gaziantep University, Gaziantep, Türkiye in 2000, 2009 and 2017 respectively. His main research interests are decision making, machine leaning, cryptology, non-invasive techniques in biomedical, image processing in textile.

HAMIYET MERKEPÇI was born on July 29th, 1979, in Gaziantep, Türkiye. She received the B.Sc. degree in mathematics from İnönü University, Malatya, Türkiye, M.Sc. degree in mathematics from Gaziantep University, Gaziantep, Türkiye and PhD. degree in mathematics from Çukurova University, Adana, Türkiye in 2002, 2009 and 2016 respectively. Her main research interests are algebra, number theory, fuzzy set, neutrosophic set, plithogenic numbers, decision making, and cryptology.

ALEXANDRA IOANID is Professor at the National University of Science and Technology POLITEHNICA Bucharest. Her research interests include entrepreneurship, marketing, business management and engineering.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/